# NAVAL POSTGRADUATE SCHOOL
## Monterey, California


# THESIS

**AN ANALYSIS OF FORENSICS EVIDENCE GATHERING FOR ASSISTANCE IN NETWORK INTRUDER PROSECUTION**

By

Steven W. Kirtley

June 1999

| | |
|---|---|
| Thesis Advisor: | Syed R. Ali |
| Associate Advisor: | Daniel F. Warren |

**Approved for public release; distribution is unlimited.**

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. AGENCY USE ONLY *(Leave blank)* | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | June 1999 | Master's Thesis |

**4. TITLE AND SUBTITLE**
**AN ANALYSIS OF FORENSICS EVIDENCE GATHERING FOR ASSISTANCE IN NETWORK INTRUDER PROSECUTION**

**5. FUNDING NUMBERS**

**6. AUTHOR(S)**
Kirtley, Steven W.

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Naval Postgraduate School
Monterey, CA 93943-5000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release; distribution unlimited.

**12b. DISTRIBUTION CODE**

**13. ABSTRACT *(maximum 200 words)***

This research develops a roadmap of legal evidence-gathering steps to assist law enforcement agencies in the identification of network intruders. This checklist will not only assist administrators in conducting network defense and safeguarding evidence but will assist them in remaining within the guidelines of the law in their network defense efforts. Legal responsibilities of network managers are highlighted with respect to legal document requirements and issues of U. S. Marine Corps liability. The aforementioned roadmap development is achieved by: 1) examining the latest advances and trends in network intrusion techniques, 2) investigating current U.S. Navy and U.S. Marine Corps Computer Network Incident Response Policies, 3) researching the current and proposed legislation covering the issue of forensic evidence requirements and preservation, and 4) examining forensics evidence gathering techniques with a focus on individual privacy rights.

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| Intrusion Detection, Forensic Evidence, Hacking, Legal Liability, Network Intrusion, Incident Response | 68 |
| | 16. PRICE CODE |

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFI- CATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UL |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

**Approved for public release; distribution is unlimited**

# AN ANALYSIS OF FORENSICS EVIDENCE GATHERING FOR ASSISTANCE IN NETWORK INTRUDER PROSECUTION

**Steven W. Kirtley**
**Major, United States Marine Corps**
**B.S., University of Florida, 1987**

**Submitted in partial fulfillment of the requirements for the degree of**

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

**from the**

**NAVAL POSTGRADUATE SCHOOL**
**June 1999**

Author: _____
Steven W. Kirtley

Approved by: _____
Syed R. Ali, Thesis Advisor

_____
Daniel F. Warren, Associate Advisor

_____ for
Reuben T. Harris, Chairman
Department of Systems Management

## ABSTRACT

This research develops a roadmap of legal evidence-gathering steps to assist law enforcement agencies in the identification of network intruders. This checklist will not only assist administrators in conducting network defense and safeguarding evidence but will assist them in remaining within the guidelines of the law in their network defense efforts. Legal responsibilities of network managers are highlighted with respect to legal document requirements and issues of U. S. Marine Corps liability. The aforementioned roadmap development is achieved by: 1) examining the latest advances and trends in network intrusion techniques, 2) investigating current U.S. Navy and U.S. Marine Corps Computer Network Incident Response Policies, 3) researching the current and proposed legislation covering the issue of forensic evidence requirements and preservation, and 4) examining forensics evidence gathering techniques with a focus on individual privacy rights.

# TABLE OF CONTENTS

## ACKNOWLEDGMENT

The author would like to acknowledge the financial support of the U.S. Marine Corps Network Operations Center (NOC), Marine Corps Systems Command, Marine Corps Combat Development Command, Quantico, Virginia and specifically Captain Carl Wright, NOC Security Manager. Thank you to my wife who spent six months as a single mother while this work was completed. Special thanks to Dr. Syed R. Ali and Daniel F. Warren for providing valuable information and guidance in carrying out this research.

# I. INTRODUCTION

## A. PURPOSE

The network intrusion rate is increasing by leaps and bounds. This is a real problem faced by all network security agencies. The U.S. Government and its agencies are no exception. Different legal bodies are working towards deterring this crime and consider it one of the top priorities on the National Security Agenda. The U.S. Marine Corps in particular does not follow an integrated methodology of evidence gathering in the network intrusion field. This thesis research develops a checklist of legal evidence gathering steps as an aid to law enforcement agencies in their investigation of network intruders. This checklist will not only assist administrators in conducting network defense and safeguarding evidence but will assist them in remaining within the guidelines of the law in their network defense efforts. Legal responsibilities of network managers are highlighted with respect to legal document requirements and issues of U. S. Marine Corps liability.

## B. BACKGROUND

U. S. Marine Corps Administrative message number 123/98 (MARADMIN 123/98) published 24 November 1998 outlined the Marine Corps' plan to migrate to the use of Windows NT for its network operating system software platform. While Windows NT is a widely used operating system it is also recognized as being very susceptible to break-in if not setup properly. Also because of its wide use Windows NT is constantly

under attack by intruders worldwide. Holes are found and exploited, and these holes are documented and quickly published on the Internet for others to easily access.

This thesis will develop a legal evidence gathering checklist to assist in the investigation of intruders. To achieve this goal we need to evaluate the latest trends in network intrusion methodology. The U. S. Marine Corps has identified a requirement to develop a specific forensic evidence checklist to assist in intruder prosecution. The model should be in the form of a roadmap containing key requirements for successful prosecution of an intruder. The checklist must contain legal steps for gathering and safeguarding evidence with attention devoted to the prevention of loss of evidence.

The checklist should facilitate the creation of a Forensic Evidence Gathering Methodology with a detailed documented timeline and stringent chain-of-custody. This documentation should then be viable for use in prosecution of computer system attackers.

## C. METHODOLOGY

The methodology will include examining the latest advances and trends in network intrusion techniques and investigating current U.S. Navy and U.S. Marine Corps computer network incident response policies. An investigation of current and proposed legislation dealing with electronic network trespassing will be conducted and applicable laws identified with a focus on individual privacy rights. A checklist will be developed of key evidence gathering steps to be conducted in the event of an intrusion incident to aid law enforcement agencies in prosecution of a network or system attacker.

The methodology used in this thesis research will consist of the following steps: 1) Conduct a literature search of books, magazine articles, applicable directives and publications, position papers, policy papers, briefings and other pertinent information resources. 2) Conduct a thorough review of major Internet sites related to actual network intrusion and hacking methods. 3) Conduct discussions with U. S. Marine Corps (USMC) Network Operations Center (NOC) personnel to determine evidence gathering procedures. 4) Conduct research of Federal and State laws to identify legal start points and information requirements. 5) Conduct a search of the Congressional Digest to identify related legislation. 6) Document the findings. 7) Work with USMC NOC security personnel to develop a checklist for forensic evidence gathering to assist law enforcement agencies in prosecution of network intruders.

## D. SCOPE

Network intrusion defense and attack is a broad subject and this research touches on a few important aspects of that subject. The specific areas of computer network hacking and the laws that apply to network intrusion, individual privacy, and organizational liability are each in themselves expansive. The scope of this thesis will be limited to U. S. Marine Corps, Department of the Navy, and Department of Defense issues and concerns. Legal issues involving evidence gathering will be limited to the Federal level and those prevalent among a majority of states within the United States of America.

## E. THESIS OUTLINE

As the use of the Internet becomes more mainstream so does hacking into business and organizational networks for pleasure or profit. This idea of conquering major computer network security systems has become associated with a David and Goliath mind frame for many, with little thought being given to the legal aspects from the both the hacker and network manager perspective. Chapter I, INTRODUCTION, provides a brief introduction to this research paper. Chapter II, BACKGROUND, discusses major legislative events affecting intrusion detection and highlights major hacking trends and current network defense mechanisms. Chapter III, INTRUDER METHODOLOGY, covers network intruder attack methodology and highlights any differences between domestic attacks and foreign attacks. Chapter IV, NETWORK INTRUSION DETECTION AND THE LAW, is an analysis of Federal and State Law relating to intruder tracing and prosecution. Chapter V, INVESTIGATIVE RESPONSIBILITIES, outlines Law Enforcement Agencies that should be involved in an investigation. Chapter VI, EVIDENCE GATHERING METHODOLOGY, reviews actual evidence gathering and evidentiary exhibit assembly. Chapter VII, INTRUSION RESPONSE CHECKLIST, will present a step-by-step guide to assist in collecting information and computer related forensic evidence in response to an identified intrusion. Chapter VII, CONCLUSION, will present conclusions and identify areas for further research.

# II. BACKGROUND

## A. HISTORY

Network managers use intrusion detection systems to detect attackers and evaluate information in order to decide on countermeasures. The methods of detection and evaluation and the countermeasures they use to combat attacks may have their own legal ramifications. These methods and the legal environment are equally complex. Technological advances clearly outpace legal change. Those involved in the legislative process are burdened with weighing the right to privacy of citizens against the need to protect critical business organization and national security assets containing vital yet vulnerable information. There are numerous Constitutional amendments with privacy implications. The First Amendment deals with freedom of speech. The Third Amendment states that during peacetime no soldier will be quartered in any house without the owners consent unless prescribed by law. The Fourth Amendment reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures, shall not be violated, and no Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." The Fifth Amendment protects against double jeopardy. The Ninth Amendment protects against slander. The Fourteenth Amendment ensures life, liberty, and property. The weight of privacy legislation makes it clear that Congress takes its duty to guarantee a citizen's right to privacy seriously. Because of legislative implications of these privacy issues and the

complexities of our communications systems the legislation which defines responsibilities for responding to a logical attack against the information infrastructure of the United States is just recently being defined.

### 1. Protecting Individual Privacy and Providing Access to Government Information

There are two aspects of individual privacy that are covered under Federal law. One is the protection of a citizen's privacy from intrusion by third parties. This covers the collection and dissemination of certain types of personal information such as medical records, financial records, arrest reports, etc. The second aspect is the protection of a citizen's privacy rights from intrusion by the government and its agencies to include law enforcement and intelligence agencies; search, seizure and surveillance. This is compounded by legislative assurances of individual access to information collected by the government.

As technological advances continue on their spiral upward, Congress finds itself continuously revisiting the issue of individual privacy weighed against information infrastructure protection. Figure 1 presents a chronological depiction of individual privacy as it relates to advances in communications technology. [1 p. 2-17]

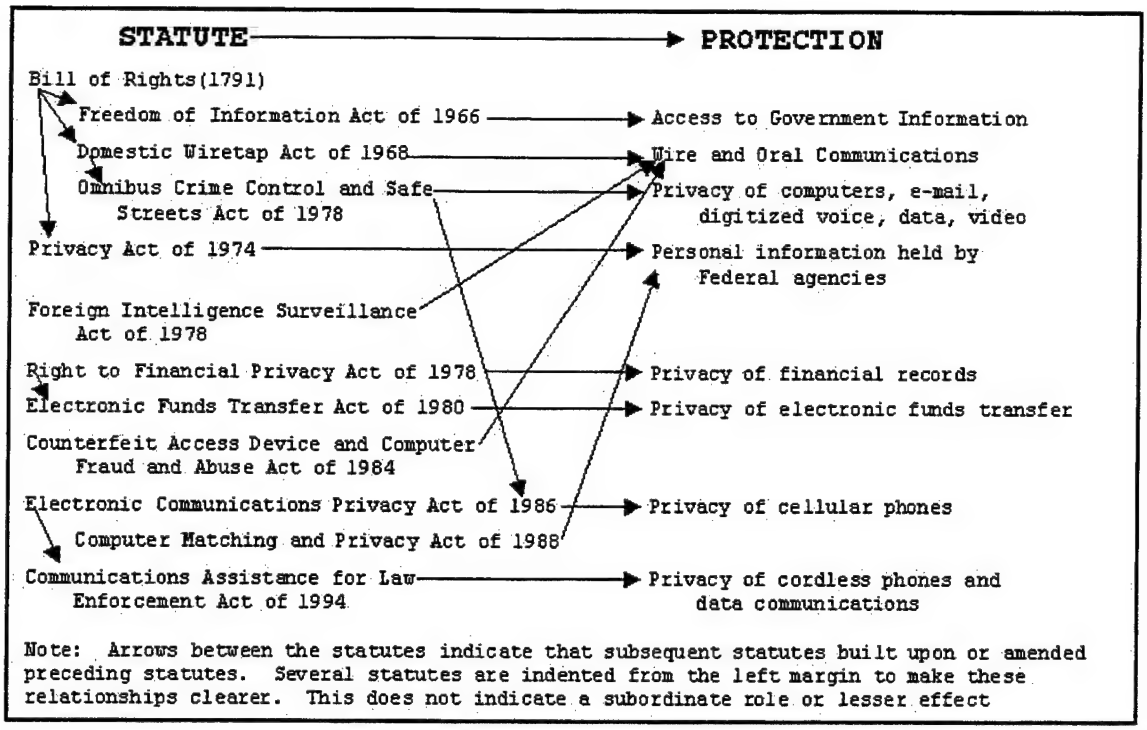


Figure 1. Privacy and Access to Government Information

## 2. Defining the Criminality of Computer Fraud and Abuse

The legal views of computer crime continue to evolve along with technology and automation, although, as stated earlier, at a slower pace. Originally, criminals using computers as a tool to commit a crime were prosecuted. Credit card fraud, for example, is a criminal act; therefore, using a stolen credit card number to buy goods over the Internet would be a crime. However, trespassing into a computer, or examining computer-generated data, without taking the data from the owner was not considered a crime. While paper documents could be stolen, stealing or unauthorized copying of computerized files and data presented perplexing legal and substantiation problems.

As communication and computer technology become more prevalent Congress continues to take action to combat computer fraud and abuse. Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, which was the first Federal computer crime legislation. The Computer Fraud and Abuse Act (CFAA) of 1986 overhauled the statute passed in 1984 and most states had made theft of computer resources a crime. [1 p. 2-25]

Even as legislation continues to catch up to technological advances in the information technology industry, Federal, state, and international jurisdictional problems arise. During the research for this paper there was no example found of a person being prosecuted for breaking into a system simply to look at files or data.

## B. HACKING TRENDS AND TECHNIQUES

With the assortment of tools available to even the most amateur hacker, Department of Defense (DoD) and United States Marine Corps (USMC) information infrastructure assets will face a continuous and increasing barrage of attacks. The USMC Network Operations Center (NOC) Intrusion Detection System (IDS) identifies an average of approximately 600 potential intrusion events that narrow down to an average of one actual incident requiring the security manager's attention per day. [17] Hackers can range from the educated and accomplished technician to the unsophisticated hobbyist out to impress friends. Typing a few key words into an Internet search engine will deliver literally thousands of web sites providing easily downloaded hacking tools, tips, and tutorials. This overabundance of readily available information coupled with the cloud of

the Internet puts the ability to conduct a sophisticated and organized attack into anyone's hands.

The rapid growth rate of the Internet increases the feasibility of computer-based attacks while decreasing the chance of trace-back. The use of jump-off sites makes it extremely difficult to identify the type of attack or to locate the attacker. An organization's increased business presence and migration to web-based applications with an emphasis on widespread connectivity provide more enticing targets for attackers. For the most part, attacks are not sophisticated works but simple exploitations of software setup errors, security oversights, or network design flaws. It is these numerous exploitations that enable hackers to penetrate systems through the use of an ever-increasing number of tools and methods.

Tremendous amounts of offensive and defensive network intrusion information are readily accessible over the Internet. The majority of this knowledge is offensive in nature and is constantly developing. As of August 1997, the Carnegie-Mellon Computer Emergency Response Team (CERT/CC) had "cataloged approximately 500 software vulnerabilities that fall roughly into two categories -- implementation errors and design errors." [2 p. 2] The consulting firm Cambridge Technology Partners, Inc. puts on a yearly network security conference where the latest hacking techniques are identified. The following items were highlighted in their May 1998 conference: [4]

- *Firewalls that run on Windows NT and Unix Servers can let hackers break into the underlying operating system via the TCP/IP protocol.*
- *HotMail, the free Internet mail service, is almost always unencrypted, making it easy for hackers to get user account names and passwords.*

- *Vulnerabilities in the Internet Protocol let malicious hackers easily install network sniffers on networks they have compromised and, unbeknownst to the user, intercept corporate data traffic.*

- *New "Smurf" attacks send echo packets from the hacker's system to the victim's via the broadcast address of a third intermediate network with a forged return address. The network is flooded with packets until it slows or crashes and it is difficult to trace the hacker.*

- *Dumpster divers, who pick through corporate garbage to find sensitive data such as passwords, are becoming more prevalent.*

- *Social engineering is calling unsuspecting computer users on a network and posing as a system administrator to get them to give away their password or other information.*
  [7 pp. 102-103]

- *Brute force attacks where script files execute rapid-fire entry of user account names and passwords until a match is made, are still used and becoming more prevalent.*

- *War dialing script files execute the systematic dialing of phone numbers within an organization to identify unprotected modems and other computers.* [7 p. 102]

- *In an FTP bounce attack, hackers manipulate FTPPASV mode using PORT and QUOTE to send scripts that allow them to gain access to unauthorized FTP servers.* [5]

- *Protocol tunneling encapsulates or hides one protocol inside another, such as a telnet inside a ping request.* [5]

- *Denial of service attacks such as, SYN flooding, ghost routing, service loops, Ping O' Death are still prevalent.* [5 and 4]

- *Viruses are showing up in the 32-bit environment and are certain to make the transition to the 64-bit platform.* [5]

As is readily apparent, computer networks will always be vulnerable to attack. As long as companies use the Internet for transferring files, sending email, downloading programs, tracking orders, tracking shipments, etc., there will always be the chance that

some malicious outsider will find a way to wreak havoc with their computer systems. But as hacking technology advances so do the tools available to combat and identify intruders.

## C. NETWORK DEFENSE THROUGH INTRUSION DETECTION

"Intrusion detection is the process of identifying and responding to malicious activity targeted at computing and networking resources." [3 p. 16] Intrusion detection is presumed to encompass the relevant technology, tools, procedures and policies used to detect malicious activity in computers and networks. It is important to keep in mind that although the target of an intruder may be a computing or networking resource, not all actions involved in the intrusion involve computing or networking resources. Remember the examples of dumpster diving and social engineering mentioned above. Most intrusion detection systems, whether network or host based, "push" alerts when they detect an event. Common methods for doing this include sending email to the system administrator, alerting a pager, or some type of alert notification on the host intrusion detection machine. These systems have serious drawbacks. Many of the alerts turn out to be false positives or false alarms. Others turn out to be simple exploit scripts that are of little consequence. The alerts become annoying to the point where they are ignored. [6 p. 1, 3 ch. 1]

Edward Amaroso in his book Intrusion Detection outlines seven basic issues in intrusion detection. [3 pp.21-34]

- The Definition of an Intrusion.
- The Methods Used by Intrusion Detection Systems.
- How Intrusion Detection Systems are Organized.
- How Intruders Hide on the Internet.
- How Intrusion Detection Systems Correlate Information.
- How Intruders Can be Trapped.
- Methods Available for Incident Response.

The problem is that intrusion is real-time while intrusion detection, evaluation, and reporting are often after-the-fact. Many hackers may be hesitant to continue in their attack efforts simply because they are being watched. If they are not hesitant, intrusion detection system audit logs are an important piece in evidence gathering methodology. The output and storage of the audit logs is of primary importance for evidence gathering in the event an intruder is successful in their attack. It is important for Network Administrators and Security Managers at all levels to understand how they work.

# III. INTRUSION TECHNIQUES

Amoroso defines an intrusion as "a sequence of related actions by a malicious adversary that results in the occurrence of unauthorized security threats to a target computing or networking domain." [3 p. 100] The problem with this definition is who decides what or who a "malicious adversary" is.

Because of the connectivity of the Internet and worldwide communications infrastructure the line between recognizing a domestic or foreign based network attack has been practically eliminated. Intruders are able to connect back-and-forth across oceans and continents with relative ease in order to cover their tracks and slow down law enforcement trace back efforts. Intruders have only to find one of thousands of available holes within a system in order to exploit the system while system administrators must protect against all available holes. Although the methodology differences between domestic attacks and foreign attacks have been completely blurred there are concerns associated with the differing attack origination locations that must be considered.

## A. DOMESTIC ATTACKS

Network managers have known for years that the most likely source of attack comes from the trusted insider. 86 percent of respondents to a recent Computer Crime and Security Survey identified disgruntled employees as likely sources of attack. 55 percent of respondents cited actual incidents of unauthorized access by insiders. [8 pp. 6-12]

Hackers are always of concern to network managers and can use the Internet or remote dial-ins as connections to gain access to internal systems. Another method on the rise is the theft of laptop computers and the compromise of their resident information to gain access.

The same study states that theft of proprietary information is perhaps the greatest threat to U.S. economic competitiveness in the global marketplace. [8 p. 5] Roughly half of network managers see U.S. business competitors as likely sources of attack on their systems with an increasing number of these attacks being linked to financial losses and financial fraud. [8 p. 5]

Serious intruder goals differ but basically involve information destruction, alteration, theft, and in some cases creation. Research shows that information thefts concentrate on passwords, financial transaction information, proprietary secrets (as stated above), customer information, and actual funds. The Department of Defense recently revised its website policy to protect against providing too much information making it harder for potential intruders or foreign agents to put together operational information. [9]

One of the latest capabilities being developed and used to combat intrusion detection systems is the coordinated attack of a system using different Internet Protocol addresses. Whether the attack is being coordinated from different computers, different locations, or addresses are being spoofed from the same computer and location, the identification process obviously becomes more difficult. Such an advanced attack would take longer to bring results to the potential intruder and presents additional audit-log record keeping and archiving issues to system managers.

## B. FOREIGN ATTACKS

System intrusions originating from foreign countries follow the same processes as mentioned above. Trace back of an intruder to their origin may take investigators through numerous jump-off points and countries before the actual origin is determined. All of these points serve to slow down or stop the investigation process but may have differing military, legal, and political issues associated with them.

Foreign competitors, just as domestic competitors, are always looking for an advantage. It is much easier to gain proprietary information through the use of system attack and information theft than to spend the money on research and development especially when the same patent laws do not apply.

Foreign governments may want to sponsor the theft of information for espionage, information warfare, and technology advancement reasons. U. S. allies have a need to gain knowledge of advanced weapons technology. Enemies want system access to lay plans to possibly disrupt communications, destroy communications infrastructure, and gain military operational information.

## C. CHAPTER SUMMARY

The portals into networks identified above coupled with the tools identified in Chapter II make a system administrator's job increasingly difficult. Protecting systems against attack is the main focus of security managers' time. The following chapters will investigate legal issues and evidence requirements when an actual intrusion is detected and law enforcement is brought in to track down the attacker.

# IV. NETWORK INTRUSION DETECTION AND THE LAW

The information age continues to produce new ways of communicating, requiring more advanced safeguards to be implemented by network security managers. Diligent intruders will overcome even the best safeguards and information will be compromised. Increasing attention is being paid to the problem of network trespassing and information theft or destruction by lawmakers. Numerous Acts have been passed in the past 25 years to deal with the advent of the information age. The Electronic Communications Privacy Act of 1986, the Computer Fraud and Abuse Act of 1986, the Computer Security Act of 1987, the Communications Assistance for Law Enforcement Act of 1994, and the Violent Crime Control and Law Enforcement Act of 1994 are acts passed by federal legislators to combat the increasing threat of computer criminals. These acts are integrated into the U.S. Code. Applicable Chapters and Sections of Title 18 of the U.S. Code can be found in their entirety at the Legal Information Institute Web Page. [12] A synopsized version is described below.

## A. FEDERAL LAW

The above mentioned legislation and other acts span various Titles and Chapters of the U. S. Code. The presentation of the following U.S. Code excerpts are important because, unlike the above mentioned Acts, Title 18 of the U.S. Code (CRIMES AND CRIMINAL PROCEDURE) specifically designates criminal violations for which an individual may be prosecuted and it highlights procedures for evidence gathering when it

involves privacy issues. Familiarity with the following basic bylaws is deemed essential in apprehending/prosecuting criminals.

### 1. Fraud and Related Activity in Connection With Access Devices

This procedure falls within section 1029 of Chapter 47 (FRAUD AND FALSE STATEMENTS) of Part 1 of Title 18 of the U.S. Code (Title 18). This section addresses laws and penalties associated with the unauthorized possession of access devices. Access device as defined in Title 18 is "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used to initiate transfer of funds (other than a transfer originated solely by paper instrument)." These devices could be wireless or otherwise but are used to knowingly defraud. It covers those who knowingly possess, traffic in, produce, or has control or custody of a "scanning receiver" or "hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services." These access devices must be used to knowingly and fraudulently obtain anything of value amounting to $1000 or more during a one-year period. Emphasis is on transactions and credit cards.

### 2. Fraud and Related Activity in Connection With Computers

This procedure falls within section 1030 of Chapter 47 of Part 1 of Title 18. This section is very applicable to network and security managers. While lengthy in its legal form, it basically says that it is against the law to knowingly access a government, financial institution, or other protected nonpublic computer with intent to defraud,

damage, extort, or obtain other protected information. It should be pointed out that intent to damage does not have to be present if unauthorized access inadvertently results in damage-to or loss-of information. This section states those damaged by unauthorized access may also seek civil damages and have two years after date of discovery of damage to file for such damages.

### 3. Procedure for Interception of Wire, Oral, or Electronic Communications

This procedure falls within Section 2518 of Chapter 119 (WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS) of PART I (CRIMES) of Title 18. This section covers procedure for applying for a court order authorizing or approving the interception of a wire, oral, or electronic communication. The section outlines required information to be included in the application for an order. It states how a judge determines the justification of such an order. The procedure outlines what information will be included in the order and the duration of such an order.

Paragraph (7) of this section contains information on when a communication may be intercepted in lieu of a court order. Paragraph (7) outlines the reasons an interception may be made based on the grounds upon which a court order is entered and the requirement to procure the order within 48 hours of the start of the interception. If the judge determines the interception was not warranted then the interception is immediately stopped and the information obtained is treated as having been obtained in violation of this chapter.

Other paragraphs cover custody and inventory of evidence, and rules for suppression of intercepted communications as well as other information.

### 4. Enforcement of the Communications Assistance for Law Enforcement Act

This procedure falls within Section 2522 of Chapter 119 of Part I of Title 18. This section basically states that if a telecommunications carrier fails to comply with a court order authorizing a communications interception under the requirements of the Communications Assistance for Law Enforcement Act the carrier may again be ordered to comply and if needed be fined up to $10,000 a day until compliance as the court may specify.

### 5. Unlawful Access to Stored Communications

This procedure falls within section 2701 of Chapter 121 (STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS) of Part I of Title 18. This section states that intentional unauthorized access of an electronic communication service facility is a crime and may result in jail time and/or fines. It further states that those, through unauthorized access, who prevent authorized access to, obtain, or alter wire or electronic communications while it is in electronic storage may also be jailed and/or fined.

### 6. Disclosure of Contents

This procedure falls within Section 2702 of Chapter 121 of Part I of Title 18. This section states those providing an electronic communications service or remote computing service to the public may not knowingly divulge the contents of a

communication while it is in electronic storage at their service facility or is carried or maintained at their service facility, except to those authorized. Those authorized to receive such communications include law enforcement agencies (with proper court documents), addressees or recipients of the communications, those with lawful consent, or those whose facilities the communication travels through to reach its destination.

### 7. Requirements for Governmental Access

This procedure falls within Section 2703 of Chapter 121 of Part I of Title 18. This section, while rife with legalese, basically states the U.S. Government must have a subpoena in order to receive access to electronic communications in electronic storage by a public provider or service or a remote computing service. While a subpoena is required the governmental agency can get not only stored communications but also telephone billing records, other subscriber telephone information, length of service of the subscriber, and types of service utilized and the government entity receiving these records is not required to notify the subscriber. This section releases the service provider from cause of action when complying with a court order to provide the above information. When a service provider is notified of an impending court ordered requirement for information they "shall take all necessary steps to preserve records and other evidence in its possession" and these records must be retained for at least 90 days and possibly 180 days when required.

### 8. Backup Preservation

This procedure falls within Section 2704 of Chapter 121 of Part I of Title 18. This section covers creation of backup copies of electronic communications and information

by the service provider as ordered by court order and the subscriber's right to challenge the governments subpoena for the records. The service provider has two days from notification by court order to complete the backup. The government entity has three days from notification by the service provider of completed backup to notify the subscriber of the court order so the subscriber may challenge the subpoena. The subscriber has two weeks to file a motion to quash the subpoena. If the subscriber makes no challenge to the court order the government entity may take receipt of the information.

**9. Delayed Notice**

This procedure falls within Section 2705 of Chapter 121 of Part I of Title 18. This section states a government entity may request an order delaying the notification of the subscriber of the court order requiring information for from 90 to 180 days. The government entity must show within its request for the court order that immediate notification of the subscriber will result in endangering the life or physical danger of an individual, flight from prosecution, destruction or tampering with evidence, witness tampering, or other actions that would jeopardize the investigation or delay the trial. The government entity must notify the subscriber at the expiration of the period of delayed notice.

**10. Cost Reimbursement**

This procedure falls within Section 2706 of Chapter 121 of Part I of Title 18. This section basically holds that a government agency requiring communications records or other information must make reasonable reimbursements to the entity assembling the documents. The reimbursement costs can include any costs due to disruption of normal

operations of any electronic communications service or remote computing service where the information was stored.

### 11. Civil Action

This procedure falls within Section 2707 of Chapter 121 of Part I of Title 18. This section states that any provider of electronic communications service, subscriber, or other person aggrieved by any violation of chapter 121 of Title 18 (and possibly other chapters) may seek civil action against those who engaged in the violation. Those victimized have two years from the time they discover or had "reasonable opportunity" to discover the violation to commence their civil action.

### 12. Counterintelligence Access to Telephone Toll and Transactional Records

This procedure falls within Section 2709 of Chapter 121 of Part I of Title 18. This section states that the Federal Bureau of Investigation may request information from a communications service provider or remote computing service provider when it applies to a person or entity believed to be involved in a foreign counterintelligence investigation or there is a belief the person or entity is a foreign power or agent. It also applies to those believed to be engaged in international terrorism or to be a foreign power or agent involved in international terrorism or violation of other criminal statutes of the United States.

Table 1 is provided as a quick reference to the above laws.

| U.S. CODE SECTION TITLE | U.S. CODE, TITLE 18, PART 1 |
|---|---|
| **Fraud and Related Activity in Connection With Access Devices** | Chapter 47, § 1029 |
| **Fraud and Related Activity in Connection With Computers** | Chapter 47, § 1030 |
| **Procedure for Interception of Wire, Oral, or Electronic Communications** | Chapter 119, § 2518 |
| **Enforcement of the Communications Assistance for Law Enforcement Act** | Chapter 119, § 2522 |
| **Unlawful Access to Stored Communications** | Chapter 119, § 2701 |
| **Disclosure of Contents** | Chapter 119, § 2702 |
| **Requirements for Governmental Access** | Chapter 119, § 2703 |
| **Backup Preservation** | Chapter 121, § 2704 |
| **Delayed Notice** | Chapter 121, § 2705 |
| **Cost Reimbursement** | Chapter 121, § 2706 |
| **Civil Action** | Chapter 121, § 2707 |
| **Counterintelligence Access to Telephone Toll and Transactional Records** | Chapter 121, § 2709 |

Table 1 - Computer Related Federal Laws

## B. STATE LAW

State laws generally fall along the same guidelines of protection as do Federal laws. There are differences from state-to-state that apply to specific needs deemed necessary by their respective legislators based upon specific incidents and trends or media reports. In addition to the previously mentioned federal computer crime related statutes, the states have also taken responsibility for developing statutory limitations specifically designed to address crime related to computers. Since 1978, when Florida became the first state to enact a computer-specific criminal statute, every other state except Vermont

has passed some form of computer-crime law. Table 2 is a limited by-state list of current computer crime related statutes. [1 p. 2-27, 9]

Table 2 - Computer Related State Laws

| U. S. STATE | PERTINENT LAWS |
|---|---|
| **ALABAMA** | Code §§ 13A-8-100 to 13A-8-103 |
| **ALASKA** | Statute §§ 11.46.200(a)(3), 11.46.484(a)(5), 11.46.740, 11.46.985, 11.46.990, 11.81.900(a)(46) & (52) |
| **ARIZONA** | Revised Statute Ann. §§ 13-2301(E), 13-2316 |
| **ARKANSAS** | Code §§ 5-41-101 to 107 |
| **CALIFORNIA** | Penal Code §§ 484j, 499c, 502, 502.01, 502.7(h), 503, 1203.047,2702 |
| **COLORADO** | Revised Statute §§ 18-5.5-101 to 18-5.5-102 |
| **CONNECTICUT** | General Statute §§ 53a-250 to 53a-261, 52-270b |
| **DELAWARE** | Code Annotated Title 11 §§ 931 to 939 |
| **FLORIDA** | State Chapters 775, 815, 934 |
| **GEORGIA** | Code Annotated §§ 16-7-22, 16-9-90 to 95 |
| **HAWAII** | Revised Statute §§ 708-890 to 896 |
| **IDAHO** | Code Title 18 Chapter 22 §§ 18-2201 to 2202, 26-1220, 48-801 |
| **ILLINOIS** | Revised Statute Chapter 38 §§ 15-1, 16D-1 to 9 |
| **INDIANA** | Code §§ 35-43-1-4, 35-43-2-3, 35-43-4-1 to 3 35-43-5-1, 35-43-7-3 |
| **IOWA** | Code §§ 716A.1 to 716A.16 |
| **KANSAS** | Statute Annotated § 21-3755 |
| **KENTUCKY** | Revised Statute Ann. §§ 434.840 to 434.860 |
| **LOUISIANA** | Revised Statute Ann. §§ 14:73.1 to 14:73.5 |
| **MAINE** | Revised Statute Ann. Title 17-A, Chapter 15, § 357, Chapter 18, §§ 431 to 433 |
| **MARYLAND** | Code Annotated §§ 27-45A, 27-145, 27-146, 27-340 |
| **MASSACHUSETTS** | General Law Chapter 266, §§ 30, 60A |
| **MICHIGAN** | Statute Annotated §§ 28.529, 752.791 to 752.797 |
| **MINNESOTA** | Statute §§ 609.87 to 609-89 |
| **MISSISSIPPI** | Code Annotated §§ 97-45-1 to 97-45-13 |
| **MISSOURI** | Revised Statute §§ 569.093 to 569.099 |
| **MONTANA** | Code Annotated §§ 45-1-205(4), 45-2-101, 45-6-310, 45-6-311 |
| **NEBRASKA** | Revised Statute §§ 28-1341 to 28-1348 |
| **NEVADA** | Revised Statute §§ 205.473 to 477, 205.481, 205.485, 205.491 |
| **NEW HAMPSHIRE** | Revised Statute Ann. §§ 638:16 to 638:19 |

| | |
|---|---|
| **NEW JERSEY** | Statute Annotated §§ 2A:38A-1 to 6, 2C:20-1, 2C:20-23 to 34 |
| **NEW MEXICO** | Statute Annotated §§ 30-16A-1 to 30-16A-4, 30-45-1 to 30-45-7 |
| **NEW YORK** | Penal Law §§ 155, 156.05, 156.10, 156.20, 156.25, to 156.27, 156.30, 165.15, 170, 175 |
| **NORTH CAROLINA** | General Statute §§ 14-453 to 13-457 |
| **NORTH DAKOTA** | Century Code §§ 12.1-06.1-01, 12.1-06.1-08 |
| **OHIO** | Revised Code Annotated §§ 2912.01, 2913.04, 2913.42, 2913.81, 2933.41 |
| **OKLAHOMA** | Statute Annotated Title 21, §§ 1951-1958 |
| **OREGON** | Revised Statute §§ 164.125, 164.377 |
| **PENNSYLVANIA** | Consolidated Statute Annotated § 3933 |
| **RHODE ISLAND** | General Law §§ 11-52-1 to 11-52-8 |
| **SOUTH CAROLINA** | Code of Law §§ 16-16-10 to 16-16-40 |
| **SOUTH DAKOTA** | Codified Law §§ 43-43B-1 to 43-43B-8 |
| **TENNESSEE** | Code Annotated §§ 39-3-1401 to 39-3-1406, 39-14-601 to 39-14-603 |
| **TEXAS** | Penal Code §§ 33.01 to 33.05 |
| **UTAH** | Code §§ 76-6-701 to 76-6-705 |
| **VIRGINIA** | Code §§ 18.2-152.1 to 18.2-152.14 |
| **WASHINGTON** | Revised Code §§ 9A.48.100, 9A.52.010, 9A.52.110, to 9A.52.130 |
| **WEST VIRGINIA** | Code §§ 61-3C-1 to 61-3C-21 |
| **WISCONSIN** | Statute §§ 943.70 |
| **WYOMING** | Statute §§ 6-3-401, 6-3-501 to 6-3-505 |

Table 2(Continued) - Computer Related State Laws

## C. CHAPTER SUMMARY

The emphasis has been on Federal Law. Laws are being passed to combat network attackers and legal loopholes are being eliminated. There are a couple of issues that need to be resolved. Does the use of an Intrusion Detection System constitute the unauthorized surveillance of communications if every communication is monitored? A government agency can request a subscriber's telephone records and communications

subscriber (Internet service provider) records. Will the websites a subscriber visits, any comments while involved in a chat or discussion group, and other information become public record if an investigation is involved?

# V. INVESTIGATIVE RESPONSIBILITIES

The importance of making face to face communications with Law Enforcement Agency personnel who will be actively investigating intrusion incidents cannot be overstated. This liaison must be made before an incident occurs so incident response team members are not leafing through phone books and calling numerous offices to try and track down a responsible person. In accordance with U.S. Navy and Marine Corps Policy, Law Enforcement Agency personnel should not be called until told to do so by Fleet Information Warfare Center (FIWC) personnel. [14 p. 8] FIWC personnel are charged with the initial investigation of a computer related incident but do not have the authority to bring charges against an attacker. Security Managers and Network Administrators should be familiar with incident reporting procedures and policies for their service.

## A. DEPARTMENT OF DEFENSE

Once an Intrusion Detection System has detected an intruder and the intrusion has been verified, users, security managers, and network managers must continue to report the incident up through their chain of responsibility. Based on direction from FIWC their first line of communication with an actual law enforcement agency may be their respective service Criminal Investigative Division (CID). Their experience with computer crime related issues may be limited but they have the necessary contacts to begin and influence the investigation. The nature of networks will almost certainly

involve interstate or international communications connections that will require the involvement of the Federal Bureau of Investigation (FBI) or possibly the U.S. Secret Service.

## B. FEDERAL BUREAU OF INVESTIGATION

The FBI's National Computer Crime Squad (NCI) investigates violations of the Federal Computer Fraud and Abuse Act of 1986. These violations involve communications that travel across multiple state or international boundaries. Violations of the Computer Fraud and Abuse Act include intrusions into government, financial, most medical, and Federal interest computers as outlined in the above sections of the U.S. Code. Federal law defines Federal interest computers as two or more computers involved in a criminal offense, which are located in different states. This would include a commercial computer that is attacked by an intruder from another state.

Computer crimes the NCCS investigates include: Intrusions of the Public Switched Network (the telephone company), major computer network intrusions, network integrity violations, privacy violations, industrial espionage, pirated computer software, other crimes where the computer is a major factor in committing the criminal offense. [10]

## C. U.S. SECRET SERVICE

The passage of the Omnibus Crime Control Act of 1984 brought to the U.S. Secret Service investigative jurisdiction for violations of Title 18 U.S. Code §§ 1029 and 1030 as outlined above and presented in more detail in the U.S. Code.

U.S. Secret Service electronic investigations have involved credit card fraud, unauthorized computer access, cellular and land line telephone service tampering, the production of false identification, counterfeit currency, threats made against the President, narcotics, illegal firearms trafficking, and even homicides. Computers are now used in the violation of virtually every crime for which the U. S. Secret Service has investigative jurisdiction. [11]

## D. STATE LAW ENFORCEMENT AGENCIES

Generally the States' Attorney General Office can be contacted to find out which Law Enforcement Agency is responsible for the investigation of computer related crime activity. [13]

# VI. EVIDENCE GATHERING METHODOLOGY

When an incident occurs where a computer or network has been compromised by an external or internal intruder, attention tends to be focused on what has been lost and how to get back into business. Computer operators, Security Managers, and System Administrators are not familiar with law enforcement requirements for actual forensic evidence. If those involved in the discovery and investigation of an intruder incident are not careful, valuable evidence may be lost more through lack of knowledge than mismanagement.

## A. INCIDENT SITE CONTAINMENT

Most of what follows in this chapter is dependent upon rapid containment of the site targeted by the intruder. The "site" may be a single computer, a server, or a group of affected computers. As the investigation of the incident progresses the "site" may expand.

### 1. Scene Snapshot

The desktop or area where the affected computer resides should be secured and any personnel, other than the system user or incident response team members, should be kept away. Attempts by self-educated experts to find and fix the problem may result in the loss of valuable data located on internal system hard drives, physical memory areas, or buffers.

Do not let anyone remove any portable storage media, such as floppy diskettes, ZIP disks, compact disks, or backup tapes, from the area. These articles should be

checked for content and viruses. If it is determined they are unaffected and safe to use a copy can be made and given to the system user so their work may continue. The original items of media should be retained by the person responsible for the incident investigation and held under a strict chain of custody.

### 2. Law Enforcement Involvement

The NAVY AND MARINE CORPS COMPUTER NETWORK INCIDENT RESPONSE Policy states that Commanding Offices or Officers in Charge will, "Report all computer network attacks/intrusion incidents against Navy and Marine Corps systems to the Fleet Information Warfare Center (FIWC) by the most expeditious means...Reports will be protected from public disclosure but classified at the lowest possible level. Unclassified reports should be marked For Official Use Only (FOUO)." [14 p. 5] This policy directive has report formats, phone numbers to FIWC and other amplifying instructions. FIWC is tasked to "man computer incident response teams that are trained and equipped to quickly respond world-wide to emerging naval computer network security incidents."[14 p. 8] While FIWC is not a recognized Law Enforcement Agency (LEA) it is clear from this policy they are to be contacted before notification of any LEA.

Once it is determined LEA involvement is required immediate contact should be made at whatever level FIWC determines. As stated in the previous chapter, it is important to maintain a familiar relationship with responsible LEA computer crime investigators in the event of their required involvement. Once they arrive on the scene they are technically in charge of the investigation. Be prepared to offer help and expertise

when appropriate and be observant to recognize whether or not they have the knowledge they require to conduct a computer crime related investigation.

## B. INTRUSION DETECTION SYSTEM (IDS) AUDIT LOGS

Audit logs or audit trails are an important piece of evidence. The processing of audit trails is not a particularly popular job with system administrators but they hold key information. To be an effective piece of evidence they must at least include the following: 1) Date, time, type, origin, and result of an auditable event; 2) Identification of the subject initiating an auditable event; 3) Identification of the object targeted by an auditable event. [3 p. 41]

### 1. Archived Logs

One of the problems with audit logs is the large size of the log and the storage duration. An organization-wide policy should be published stating archiving duration and methods. Because of the enormous size of audit logs they will certainly have to be compressed when stored. If possible, logs should be authenticated before and after compression with a software program that assigns an algorithmic hash or other electronic signature to the file as a signature of its authentication, guaranteeing it has not been altered.

## C. HARD DRIVES

System hard drives may be a critical system asset to some organizations. Original hard drives from affected systems should be labeled and placed in an access controlled safe. Investigators or LEA typically may get by with a copy of any hard drive data from

an affected system but would prefer and may require the original for the investigation. Having the capability to make a mirror copy of your hard drive will assist in efforts to get the affected system back on-line. Experts recommend that two backups be made and if possible a backup be used for the investigation. Two backups are recommended in case LEA personnel or other investigators lose evidence or the chain of custody is compromised. There are numerous methods to replicate your hard drive.

### 1. Drive Duplicator

Drive duplicators are a piece of hardware available on the market that do just what they advertise. They are advertised as fast and reliable but have not been used as a forensics tool. [15 p. 67]

### 2. Backups

A hard drive backup can be performed using a new unopened disk or tape. The media should be capable of holding all information on the drive. Again, it is very important the media be new and not previously used. Some analysis techniques are so sophisticated they will recognize shadows of bits that have been overwritten.

### 3. Bit-By-Bit Copy

Making a bit-by-bit backup copy of your hard drive is better for forensics. This copy will identify and record all bit spaces on the hard drive, which may include malicious code or files that were used by the attacker and deleted. The pointers to the code and/or files are deleted but the file/code information may still reside on the hard drive. Smart attackers can do more than just overwrite data; they can encrypt and hide it. They may try to hide their work by marking cluster as bad on the disk, hiding information

inside TCP header fields crossing a network, and hiding files inside files. [15 p. 174] All of these areas can be investigated if there is a bit copy of the drive.

## D. INTERNAL INCIDENT

As identified in Chapter 3, 55 percent of respondents to a 1999 computer crime and security survey reported unauthorized access to systems by insiders. When an insider wages an attack there will be at least two physical areas to be secured and investigated. A system attack conducted by an organization insider brings with it additional concerns and requirements.

### 1. Conventional Forensics

Conventional forensics involves the gathering of evidence that may not be computer related. When an internal attacker is identified, he or she should be asked to stop typing and to move away from their keyboard. The area should be secured as mentioned above but with additional attention paid to other sources of trace evidence. They may want to try and determine if someone else, other than the primary user, used the computer system to launch the attack. Investigators may want to try and remove fingerprints from computer hardware. They may want to try and collect clothing, hair, skin, and other types of fragmented trace evidence from furniture and flooring. The following is an example of the importance of preserving internal attacker evidence, "Adelyn Lee won a $160,000 civil case for wrongful dismissal from Oracle Corporation, but a subsequent investigation revealed that she had performed unauthorized access on

her supervisor's email account and generated the evidence used to win her civil liability case." [8 p. 6]

### 2. Portable storage media

All portable storage media found in the area of a system computer identified as one used by an internal attacker should be collected, labeled, and maintained in a strict chain of custody. This media can be checked for malicious code or other pertinent evidence in the course of the investigation.

## E. HISTORICAL RECONSTRUCTION

Those who have not been the victim of a network computer attack that has been investigated and gone to actual trial do not realize that it normally takes over two years from the time of the incident to actual prosecution of the intruder. For this reason it is important to be able to accurately reconstruct events surrounding the incident.

### 1. Written Notes

Written notes should be taken from the beginning of an incident discovery or notification. Write the notes in the manner of log book entries keeping a time line and being as detailed as possible. These notes could very well be admitted as evidence in court and should be retained under a chain of custody in the same manner as other evidence. [15 p.13] Notes should be detailed enough to be able to refresh an investigators memory two years after the fact. Imagine trying to answer detailed questions from a lawyer based on information you remember from reviewing your notes.

### 2. Audio Tape

If the scenario precludes an investigator or response team member from taking written notes, it is a good idea to use a small cassette tape recorder to verbally record your notes for later transcription. Be detailed and try to maintain a timeline. Keep the tape or tapes under the same chain of custody as you do with other evidence.

### 3. Video Tape

If warranted a video recording of the scene may be taken. If deemed appropriate a video recording of the scene from discovery of the incident until investigation completion may be made. The video would contain who came into the area, what exactly was on the computer screen, and could be referred to at later dates to clarify questions or corroborate evidence. Keep the tape or tapes under the same chain of custody as you do with other evidence.

## F. EVIDENCE ASSEMBLY

All evidence gathering mentioned above is expected to be done by Security Managers, System Administrators, or Incident Response Team Members in anticipation of arrival of a FIWC Incident Response Team or LEA investigative personnel. Once on site FIWC and LEA personnel are supposed to have requisite knowledge and procedures for collection and safekeeping of evidence. Until they arrive it is important that any hardware, software, data, or other materials gathered be safeguarded.

### 1. File Authenticity

File authenticity will become an issue in court. The importance of an organization's network systems will determine how much attention and money the organization is willing to spend on protecting them. Software programs such as "Tripwire" exist to verify file authenticity. Tripwire is an integrity monitor for Unix systems. It uses several checksum/message-digest/secure-hash/signature routines to detect changes to files, as well as monitoring selected items of system-maintained information. The system also monitors for changes in permissions, links, and sizes of files and directories. It can be made to detect additions or deletions of files from watched directories. The configuration of Tripwire is such that the system/security administrator can easily specify files and directories to be monitored or to be excluded from monitoring, and to specify files that are allowed limited changes without generating a warning. Tripwire can also be configured with customized signature routines for site-specific checks. Tripwire, once installed on a clean system, can detect changes from intruder activity, unauthorized modification of files to introduce backdoor or logic-bomb code, and virus activity (if any were to exist) in the Unix environment. This software was developed at Purdue University and is free to download from their File Transfer Protocol (FTP) site. [16] Software packages exist that do the same thing for other operating systems.

### 2. Chain of Custody

The importance of the chain of custody cannot be overemphasized. To develop a sound chain of custody talk to the organization's legal counsel about the specimen chain

of custody for the command urinalysis program. There should be a responsible officer or person with very stringent guidelines on who is to handle evidence, how it is to be handled, how it is to be recorded and signed for, and where it is to be kept. Access to evidence should be granted to only the "privileged" few connected to the incident investigation when there is a need for access. Be sure to receive signatures from LEA personnel if and when they arrive to take possession and give a follow-up call to ensure "everything is going well on their end." In other words you may want to call periodically to ensure evidence has not been lost.

## G. CHAPTER SUMMARY

Remember that evidence gathered must be admissible in court. These cases are very complex and technical so evidence must be relevant. Real evidence are the tangible items, the seized computer, the diskettes, the audit logs. Direct evidence comes from what the investigator actually saw – not surmised. Submitted evidence should be reliable and paint a picture that leads to a decision; not a hung jury and a case that may have to be tried again. [15 p. 142-143]

All evidence collected is made available to the defense during discovery before the trial. Good evidence collection and detailed notes and recollections will make it easier to prepare the case and harder for the defense to find holes.

## VII. EVIDENCE GATHERING CHECKLIST

Preparation is crucial to successful intusion response. A well organized incident response policy is important. [15] Those responsible for incident response and recovery must be prepared with established procedures such as the following checklist.

### A. EVENTS LEADING TO EVIDENCE GATHERING

#### 1. Determine That There is an Actual Intrusion Event.

Take appropriate actions to determine whether an actual network intrusion has occurred. Make sure a virus or other type of malicious code was not introduced to the computer through a floppy disk or other means. It is important to be mindful of all evidence gathering activities and to continue the investigation to determine if the intrusion came from inside or outside the organization.

#### 2. Keep Actions Low Key.

Do not cause an uproar. There is probably no need to have a command wide notification of the incident. Notify only those within the organization with a legitimate need to know.

#### 3. Notify Commander or Officer-in-Charge.

Always keep them informed. There may be a requirement to get their authorization in order to bring down the network if required. They will want to keep their superiors informed.

**4. Do Not Turn Off Computer.**

Valuable forensic evidence of intruder activity located in caches, buffers, and random access memory will be lost if the computer is turned off.

**5. Disconnect Affected Computer from the Network.**

Simply unplug the computer from the network. There are problems this may create depending on the type of network configuration the organization has but the problems created are easier to deal with than the compromise of other computers.

**6. Secure the Immediate Area without Disrupting Other Operations.**

If possible cordon off the area. Keep personnel not involved in the incident investigation out of the area. Do not let any self-educated computer engineers attempt to troubleshoot the system. Maintain control of all articles in the immediate area especially portable storage media like floppy disks, Zip disks, Compact Disks (CD), data tapes, etc.

**7. Take Detailed Notes of all Actions Taken and Occurrences.**

Start taking notes as soon as possible. Establish a timeline and be as detailed as possible. If available use a new note tablet or log book of some kind that can be devoted specifically to the incident

**8. Have an Assigned Responsible Person begin Gathering Information for the Required Incident Report to FIWC.**

OPNAV INSTRUCTION 2201.2 requires units experiencing computer network incidents to send a report to FIWC. [14 pp. 6-7] Notify FIWC as soon as practical and determine if outside Law Enforcement Agency involvement is required.

## B. EVIDENCE GATHERING METHODOLOGY

### 1. Establish Chain of Custody.

Take responsibility or assign someone as the responsible person for maintaining control of any evidence gathered to include notes.

### 2. Make a Videotape of the Area and Evidence Gathering Activities.

If possible, make a videotape of the affected computer and what specifically was on the screen and the surrounding area. If practical continue to videotape the evidence gathering activities keeping in mind the tape may be admissible in court.

### 3. Gather any Portable Storage Media.

Collect and label with date, time, location, and owner's name any portable storage media in proximity to the affected computer. If any disks, CDs, or tapes are required for operations to continue, check them for malicious code and make a copy to be used for operations. Log the media into the chain of custody.

### 4. Make a Copy of the Computer Hard Drive.

If possible make a bit-by-bit copy of the affected hard drive. If unable to do this, make a standard backup of the drive.

### 5. If the Expertise Exists try to Copy the Contents of the Computer's Random Access Memory, Caches, and Buffers.

To date, no simple standard capabilities exist to do this within the computer security community but efforts are under way to try and develop software that will accomplish this task. [15 p. 174]

### 6. Turn Off Computer and Remove Hard Drive.

Once all copies have been made, turn off the computer and remove the hard drive and introduce it into the chain-of-custody. If there was operational dependent information on the hard drive scan one of the backup copies for malicious code and use it on a new hard drive.

### 7. Be Careful of Trace Evidence if Internal Incident.

Investigators may be interested in trace evidence specimens such as fingerprints, hair and cloth fibers, scratches, etc., when looking at an intrusion incident conducted by an employee internal to the organization. Again, it is important to be mindful of all evidence gathering activities and to continue the investigation to determine if the intrusion came from inside or outside the organization.

### 8. Introduce All Evidence into Chain-of-Custody and Secure It in a Controlled Place.

The evidence should be put inside a secure container and locked away. To put it in a box and put it in a desk or uncontrolled room is not enough. Keep in mind the example of the urinalysis chain-of-custody. If possible put in a lockable box and put in a controlled safe or room. This evidence will be turned over to Law Enforcement Personnel in the course of an investigation.

### 9. Go Over the Notes.

Take time to pay attention to the notes detailing the incident and the evidence gathering activity. Make them as detailed as possible. If this incident's intruder goes to trial they will have to paint a picture up to two years later.

## C. FOLLOW UP

### 1. Get Operations Back On Line.

Perform the required actions to get the network operational.

### 2. Conduct an After Action Review.

Conduct a review of organizational network security measures to determine how the intruder got in. If the intrusion was by an insider review internal policies. Review incident response procedures and evidence gathering techniques and capabilities. Identify needed corrections and required capabilities for the future.

### 3. Make Corrections to Network Security to Fill Identified Holes and Continue to Monitor.

Once the network holes are identified make the corrections or fixes and monitor the network more closely for a period of time.

## D. CHAPTER SUMMARY

This chapter provides a step-by-step checklist of actions to perform once a computer has been identified as compromised. Appendix A is provided as a checklist for organizational use.

# VIII. CONCLUSION

## A. CONCLUSION

Network security is a challenge that is ever changing and getting more complex every day. This Thesis deals with forensic evidence gathering methodology at the organizational level to assist Law Enforcement Agencies in the prosecution of a detected network attacker. The methodology included exploring the latest advances and trends in network intrusion techniques and researching current U.S. Navy and U.S. Marine Corps computer network incident response policies. Current and proposed legislation dealing with electronic network trespassing was reviewed and applicable laws identified with a focus on individual privacy rights. A checklist was developed of key evidence gathering steps to be conducted in the event of an intrusion incident to aid law enforcement agencies in prosecution of a network or system attacker.

## B. RECOMMENDATIONS

Organizations should research and establish a Network Intrusion Incident Response Plan to be implemented at all levels where unauthorized network access can be gained by an outside entity.

A Network Intrusion Incident Response Person or Team should be assigned and educated on incident response methodologies, technologies, and governmental policies.

All network computer users should be educated on immediate incident response measures to be taken in the event they suspect their computer has been compromised in order to assure valuable evidence is not lost.

## C. AREAS FOR FURTHER STUDY

Network Administrators should be educated on the legal issues surrounding the limits of liability of an organization whose computer network is used as a jump-off point for an attacker causing massive damage to another organizations system. This is to prevent loss of not only monetary physical/data assets but also public confidence. Organizational legal guidelines should evolve in accordance with the ever-changing code of law for computer crime prevention. Further study is recommended to develop a training course based on the facts discussed in this thesis as guidelines.

The issue of whether intrusion detection monitoring of all system traffic equates to wiretapping has not been resolved. Court cases have found that banner warnings are both sufficient and insufficient, as a warning of monitoring of system traffic. There is a requirement for research into which state and Federal courts uphold electronic banners as sufficient warning of monitoring activity.

There exists a need in the forensic evidence gathering community for a piece of software that can be introduced into an affected computer that will make a bit-by-bit copy of all internal memory systems within the computer to include the buffers, caches, and random access memory.

## LIST OF REFERENCES


1. Joint Pub 1, INFORMATION WARFARE, Legal, Regulatory, Policy and Organizational Considerations for Assurance, 4 July 1995.

2. *Proceedings From the Carnegie Mellon Workshop on Network Security,* Scientific and Technical Intelligence Committee, Director of Central Intelligence, August 1997.

3. Edward Amoroso, *Intrusion Detection, An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response*, Intrusion.Net Books, January 1999.

4. Laura DiDio. *Closing those open doors*. Computerworld, June 1, 1998. http://www.computerworld.com/home/print.nsf/all/9806014D22

5. Jacqueline Emigh, *Network Cracking Turns Meaner With Fracking...,* Newsbytes, May 28, 1998. http://www.jammed.com/Lists/ISN/1998-May/ISN-182

6. Vicki Irwin, Stephen Northcutt, and Bill Ralph. *Building a Network Monitoring and Analysis Capability-Step by Step*, SANS Institute, 1998. http://www.nswc.navy.mil/ISSEC/CID/step.htm

7. Carolyn P. Meinel, *How Hackers Break In...and How They Are Caught,* Scientific America, October 1998.

8. Richard Power, *1999 CSI/FBI Computer Crime and Security Survey,* Computer Security Issues & Trends, Computer Security Institute, Vol. V, No. 1, Winter 1999.

9. LEXUS/NEXUS Online legal research system.

10. Federal Bureau of Investigation National Computer Crime Web Page. http://www.emergency.com/fbi-nccs.htm

11. United States Secret Service Web Page, Financial Crimes Division. http://www.treas.gov/usss/financial_crimes.htm#Electronic%20Crime%20Branch

12. Legal Information Institute U.S. Code Web Page, Table of Contents. http://www4.law.cornell.edu/uscode/index.htm

13. Interview with Stephen Northcutt, Incident Handling Research Program Director, System Administrators and Network Security (SANS) Institute, 1999 SANS Conference, Baltimore MD, May 13, 1999.

14. NAVY AND MARINE CORPS COMPUTER NETWORK INCIDENT RESPONSE, OPNAV INSTRUCTION 2201.2, 3 MAR 1998.

15. Incident Handling: Step-by-Step and Computer Crime Investigation Course, System Administrators and Network Security (SANS) Institute, 1999 SANS Conference, Baltimore MD, May 13, 1999.

16. Tripwire was written as a project under the auspices of the COAST Project at Purdue University. The primary author was Gene Kim, with the aid and under the direction of Gene Spafford (COAST Director).
ftp://coast.cs.purdue.edu/pub/COAST/Tripwire

17. Interview with U.S. Marine Corps Network Operations Center Personnel, Marine Corps Combat Development Command, Quantico, Virginia, 18 February 1999

## APPENDIX A. EVIDENCE GATHERING CHECKLIST

### EVENTS LEADING TO EVIDENCE GATHERING

1. **Determine That There is an Actual Intrusion Event.**

   Determine whether or not virus/malicious code was introduced. Determine the origin (internal/external) of the intrusion.

2. **Keep Actions Low Key.**

3. **Notify Commander or Officer-in-Charge and Only Those Within the Organization with a Need to Know.**

4. **Do Not Turn Off Computer.**

5. **Disconnect Affected Computer from the Network by Simply Unplugging the Computer from the Network.**

6. **Secure the Immediate Area Without Disrupting Other Operations.**

7. **Record Detailed Notes of all Actions Taken and Occurrences as Soon as Possible in a Logbook.**

8. **Have an Assigned Responsible Person Begin Gathering Information for the Required Incident Report to FIWC per OPNAV INSTRUCTION 2201.2**

   Query FIWC to determine if outside Law Enforcement Agency involvement is required.

### EVIDENCE GATHERING METHODOLOGY

1. **Establish Chain of Custody.**

   Take responsibility or assign someone to maintain control of any evidence gathered to include notes.

2. **Make a Videotape of the Area and Evidence Gathering Activities.**

3. **Gather any Portable Storage Media.**

   Collect and label with date, time, location, and owner's name any portable storage media in proximity to the affected computer. Check them for malicious code and make a copy to be used for operations. Log the media into the chain of custody.

4. **Make a Copy of the Computer Hard Drive.**

   If possible make a bit-by-bit copy of the affected hard drive. Otherwise, make a standard backup of the drive.

5. **If the Expertise Exists Copy the Contents of the Computer's Random Access Memory, Caches, and Buffers.**

   This capability is not established within the computer security community but efforts are under way to try and develop software that will accomplish this task.

6. **Turn Off Computer and Remove Hard Drive Only When All Copies Have Been Made.**

7. **Be Careful of Trace Evidence if it is an Internal Incident.**

8. **Introduce All Evidence into Chain-of-Custody and Secure It in a Controlled Place.**

9. **Go Over the Notes Taking Time to Pay Attention to the Notes Detailing the Incident and the Evidence Gathering Activity. Make Them as Detailed as Possible.**

<u>FOLLOW UP</u>

1. **Get Operations Back On Line.**

   Perform the required actions to get the network operational.

2. **Conduct an After Action Review of Organizational Network Security Measures to Determine How the Intruder Got In. Identify Needed Corrections and Required Capabilities for the Future.**

3. **Make Corrections to Network Security to Fill Identified Holes and Continue to Monitor.**

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center ..... 2
   8725 John J. Kingman Rd., Ste 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library ..... 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5000

3. Dr. Syed R. Ali, DISA Chair, Code CC/SA ..... 2
   Naval Postgraduate School
   Monterey, California 93943-5000

4. Dan Warren, Code CS ..... 2
   Naval Postgraduate School
   Monterey, California 93943-5000

5. LtCol Terrance Brady USMC, Code IS/BA ..... 1
   Information Operations Academic Group
   Naval Postgraduate School
   Monterey, California 93943-5000

6. Carl Wright, Security Manager ..... 2
   U.S. Marine Corps Network Operations Center
   Marine Corps Combat Development Command
   Quantico, Virginia 22134